The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
9/8/2009

SUBJECT:
Vulnerabilities in Windows Media Format Runtime Could Allow Remote Code Execution (MS09-047)

OVERVIEW:
Two vulnerabilities have been discovered in the Windows Media Format Runtime that could allow a remote attacker to take complete control of a vulnerable system. The Windows Media Format Runtime provides information to applications, such as Windows Media Player. These vulnerabilities can be exploited if a user visits a malicious web page or opens a malicious media file. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Windows 2000
- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008

RISK:

Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
Two vulnerabilities have been discovered in the Windows Media Format Runtime that could allow a remote attacker to take complete control of a vulnerable system. The vulnerabilities occur when Windows processes an Advanced System Format (ASF) file with malformed headers or an MPEG-1 Audio Layer 3 (MP3) file with specially crafted metadata. ASF files may have a number of different extensions, including .ASF, .WMV, or .WMA.

When a client application, which utilizes the Windows Media Format Runtime, processes a specially crafted file, exploitation may occur. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply the appropriate patch provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to open email attachments from unknown or un-trusted sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Consider blocking ASF, WMV, WMA, and MP3 files at the network perimeter.

REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/Bulletin/MS09-047.mspx
http://blogs.technet.com/srd/archive/2009/09/08/assessing-the-risk-of-the-september-critical-security-bulletins.aspx

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2498
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2499

Security Focus:
http://www.securityfocus.com/bid/36225
http://www.securityfocus.com/bid/36228